

CS556 Introduction to Cryptography - Prof. Ming-Deh Huang
 Scribe: Iftikhar A Burhanuddin
 burhanud@usc.edu
 Class #5 and #6 - September 10 and 12, 2002

Announcements:

Lecture notes for class #4 are online. We'll finish our Chapter 1 discussions and start Chapter 3 and come back to Chapter 2 later.

Topics for today:

1. $\phi(n)$ and the Chinese Remainder Theorem
2. An interesting identity
3. Caesar Cipher and Digraphs
4. Matrix ciphers

1. $\phi(n)$ and the Chinese Remainder Theorem

Last time we learnt how to solve a system of modular linear congruences under a very general condition using the Chinese Remainder Theorem.

Given moduli m_1, \dots, m_k such that $(m_i, m_j) = 1$ for all $i \neq j$ and $a_1, a_2, \dots, a_k \in \mathbf{Z}$, $\exists!$ solution to (*) modulo $M = \prod_{i=1}^k m_i$

$$(*) = \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

In other words the following map is a bijection.

$$\begin{array}{ccccccc} \mathbf{Z}/M\mathbf{Z} & \rightarrow & \mathbf{Z}/m_1\mathbf{Z} & \times & \mathbf{Z}/m_2\mathbf{Z} & \dots & \mathbf{Z}/m_k\mathbf{Z} \\ x & \mapsto & (x \pmod{m_1}, & & x \pmod{m_2}, & \dots, & x \pmod{m_k}) \end{array}$$

Once the moduli are fixed \rightarrow is clearly true. CRT gives us the \leftarrow direction by saying that the remainders determine x uniquely. Hence this map gives a way to break down the identity of x into pieces.

Ex: $M = 6 = 2 * 3$

$$\begin{array}{rcl}
 \mathbf{Z}/6\mathbf{Z} & \rightarrow & \mathbf{Z}/2\mathbf{Z} * \mathbf{Z}/3\mathbf{Z} \\
 0 & \mapsto & (0, 0) \\
 4 & \mapsto & (0, 1) \\
 2 & \mapsto & (0, 2) \\
 3 & \mapsto & (1, 0) \\
 1 & \mapsto & (1, 1) \\
 5 & \mapsto & (1, 2)
 \end{array}$$

Say $(m, n) = 1$ then the following map is a bijection

$$\mathbf{Z}/mn\mathbf{Z} \rightarrow \mathbf{Z}/m\mathbf{Z} * \mathbf{Z}/n\mathbf{Z}$$

We are interested in ascertaining whether the ϕ function is multiplicative. Recall that $\phi(N)$ is defined to be the cardinality of the set of numbers prime to N , i.e. $|\mathbf{Z}/N\mathbf{Z}^*|$.

$$\begin{array}{rcl}
 \phi(mn) & =? & \phi(m) * \phi(n) \\
 \parallel & & \parallel \\
 \Leftrightarrow |\mathbf{Z}/mn\mathbf{Z}^*| & =? & |\mathbf{Z}/m\mathbf{Z}^*| * |\mathbf{Z}/n\mathbf{Z}^*|
 \end{array}$$

Next we claim that a map involving multiplicative groups is a bijection which would imply that ϕ is multiplicative.

Claim: The following map with $\gcd(m, n) = 1$ is a bijection

$$\mathbf{Z}/mn\mathbf{Z}^* \rightarrow \mathbf{Z}/m\mathbf{Z}^* \times \mathbf{Z}/n\mathbf{Z}^*$$

Proof: If $\gcd(x, mn) = 1 \Rightarrow \gcd(x, m) = 1$ and $\gcd(x, n) = 1$ and the map is injective (one-to-one).

Suppose $(a_1, a_2) \in \mathbf{Z}/m\mathbf{Z}^* \times \mathbf{Z}/n\mathbf{Z}^*$, that is $\gcd(a_1, m) = \gcd(a_1, n) = 1$. CRT tell us that there exists an x such that $x \equiv a_1 \pmod{m}$ and $x \equiv a_2 \pmod{n}$. Moreover, the former congruence implies that $\gcd(x, m) = \gcd(a_1, m) = 1$ and the latter implies that $\gcd(x, n) = \gcd(a_2, n) = 1$. So $\gcd(x, mn) = 1$. And we've proved the surjective (onto) nature of the map and therefore the bijectivity. \diamond

A corollary to the claim is the if $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m) * \phi(n)$.

Remark: Consider a number N which is a product of two primes p, q . How big is the group $\mathbf{Z}/N\mathbf{Z}^*$? Now we know that $|\mathbf{Z}/N\mathbf{Z}^*| = \phi(N) =$

$\phi(p)\phi(q) = (p-1)(q-1)$. Also the fraction of numbers between 1 and $n-1$ which are relatively prime to N is $\frac{\phi(N)}{N} = \frac{(p-1)(q-1)}{pq} = (1 - \frac{1}{p})(1 - \frac{1}{q})$. In case the primes are *very big*, their reciprocals are very small and $(1 - \frac{1}{p})(1 - \frac{1}{q})$ is very close to 1. This is a non-trivial fact that is leveraged in the RSA cryptosystem. The rationale is that as almost all numbers can be encoded the system has a negligible chance of being broken (by computing appropriate gcd and recovering the factors of N). Imagine the (in)security guaranteed by a cryptosystem where 1 out of every 1000 numbers is not encodable!

2. An interesting identity

$$n = \sum_{d|n} \phi(d)$$

is proved by using the fact that ϕ is multiplicative in the textbook [NK] and a HW problem [NK, I.3.22] asks you to prove it by looking at the subgroups of $\mathbf{Z}/N\mathbf{Z}$. Here's an outline which should help you with your HW I.

$\langle a \rangle = \langle \gcd(a, n) \rangle$. For $d|n$ define $S_d := \langle \frac{n}{d} \rangle$. Observe that $n = \sum_{d|n} (\# \text{ generators for } S_d)$ as any element cannot generate two different subgroups and hence we are counting each number in $\{1, \dots, n\}$ once and only once. Moreover as $\langle i \frac{n}{d} \rangle = S_d \Leftrightarrow \gcd(i, d) = 1$ this implies that $\#$ of generators of $S_d = \phi(d)$ and the identity follows.

3. Caesar Cipher and Digraphs

We can generalize the Caesar scheme ($E(x) = x + a \pmod N$) to $E(x) = ax + b \in \mathbf{Z}/N\mathbf{Z}$. Now to be a good encryption scheme $E(x)$ needs to be a bijection.

Claim: $E(x)$ is bijective iff $\gcd(a, N) = 1$.

Proof: Say $y = ax + b \Leftrightarrow x = a^{-1}(y - b) \pmod N$. And as we know a^{-1} exists and is unique iff $\gcd(a, N) = 1$ \diamond

The encryption key for this scheme is (a, b) and the number of choices for the key are $\phi(N) * N$, which is definitely an improvement over the Caesar which has only N key choices.

Let's consider digraphs which are an alternative representation of pairs of

letters.

$$\begin{array}{ccc} \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z} & \rightarrow & \mathbf{Z}/N^2\mathbf{Z} \\ (i, j) & \mapsto & i * N + j \end{array}$$

For example take $N = 26$

$$\begin{array}{ccc} \mathbf{Z}/26\mathbf{Z} \times \mathbf{Z}/26\mathbf{Z} & \rightarrow & \mathbf{Z}/26^2\mathbf{Z} \\ (3, 4) & \mapsto & 3 * 26 + 4 \end{array}$$

Enciphering using $E(x) = ax + b$ where $a, b \in \mathbf{Z}/26^2\mathbf{Z}$ we see that the number of choices of keys is $\phi(n^2) * N^2$. So the advantage of digraphs seems to be that more attempts have to be made to break the scheme using a brute force attack. But looking more closely we see that there's an inherent weakness.

Suppose $x = iN + j$ so $E(x) = ax + b = a(iN + j) + b = aiN + (aj + b)$ in $\mathbf{Z}/26^2\mathbf{Z}$. If an adversary Eve can compute $E(x)$ modulo $N = (aj + b) \bmod N$ we see that $E(x)$ modulo N is a function of j and not i . So by performing frequency analysis on the even positions (the j 's) Eve will be able to compute $a \bmod N$ and $b \bmod N$. Though Eve doesn't have complete information about $a \bmod N^2$ and $b \bmod N^2$ she still has a lot of information to make digraphs succumb to this type of attack.

4. Matrix ciphers

If we think of (i, j) as a vector we can construct another scheme by working with 2-dimensional matrices over $\mathbf{Z}/N\mathbf{Z}$

$$M_2(\mathbf{Z}/N\mathbf{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbf{Z}/N\mathbf{Z} \right\}$$

The next encryption function we consider is $E(x) = Ax + b$ where $A = M_2(\mathbf{Z}/N\mathbf{Z})$ and $b \in (\mathbf{Z}/N\mathbf{Z})^2$. Again we'll require that E should be a bijection and this is the case iff the matrix A is invertible which directly follows from what we know about matrices over the reals. Next we'll present a necessary and sufficient condition for a matrix $\mathbf{Z}/N\mathbf{Z}$ to be invertible.

Remark:

1. Most results we'll derive apply in general to arbitrarily sized matrices though we are primarily interested in the 2x2 case.

2. Note that all operations involving elements of the matrices happen in $\mathbf{Z}/N\mathbf{Z}$.

Claim: Given a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}/N\mathbf{Z})$ and $\det(A) \in \mathbf{Z}/N\mathbf{Z}^*$ we can compute $B = \begin{pmatrix} u & v \\ w & x \end{pmatrix} \in M_2(\mathbf{Z}/N\mathbf{Z})$ such that

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (**)$$

Proof: From (**) we get 4 equations in 4 unknowns and we'll work with the following two: $au + bw = 1$ (i), $cu + dw = 0$ (ii). Multiplying (2) by b and subtracting it from (i) times d , we eliminate w and obtain $u = (\det(A))^{-1} \cdot d$ and solving for the other unknowns we can compute B . \diamond

Remark: The above argument tells us that we can perform Gaussian elimination to compute the inverses in $M_2(\mathbf{Z}/N\mathbf{Z})$ if one exists.

Lemma: The map $E : x \mapsto Ax + b$ is a bijection iff A is invertible

Proof: The map is clearly injective. Say $y = Ax + b$ and suppose A is invertible. Then this implies $y - b = Ax \Rightarrow x = A^{-1}(y - b)$ and the map is surjective. Conversely if E is bijective we want to show that A has an inverse, that is we can construct a B such that $AB = I$. Suppose $B = \begin{pmatrix} u & v \\ w & x \end{pmatrix}$. Viewing the matrix B as a set of two column vectors gives us the following equations

$$A \begin{pmatrix} u \\ w \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } A \begin{pmatrix} v \\ x \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

As the encryption map E is bijective we get

$$A \begin{pmatrix} u \\ w \end{pmatrix} + b = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \text{ and } A \begin{pmatrix} v \\ x \end{pmatrix} + b = \begin{pmatrix} 0 \\ 1 \end{pmatrix} + b$$

which in turn implies that

$$\exists! \begin{pmatrix} u \\ w \end{pmatrix} \text{ such that } E \begin{pmatrix} u \\ w \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b$$

$$\text{and } \exists! \begin{pmatrix} v \\ x \end{pmatrix} \text{ such that } E \begin{pmatrix} v \\ x \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} + b$$

Hence there exists a unique matrix B such that $A.B = I$ \diamond

Remark: Recall that in the case of matrices over the reals (or the rationals), a matrix is invertible iff its determinant is non-zero which is equivalent to saying that the determinant is invertible over the reals (or the rationals). Similarly in our case matrix A is invertible iff $\det(A) \in \mathbf{Z}/N\mathbf{Z}^*$.

This completes the proof of $E(x)$ is a bijection iff A is invertible iff $\det(A) \in \mathbf{Z}/N\mathbf{Z}^*$

The # of possible keys seem to be N^6 but A is not arbitrary matrix but an invertible one. So we can think about the following:

1. What is the size of the key space?
2. Eve needed one plaintext-ciphertext pair to break the original caesar cipher system. How many such plaintext-ciphertext pairs does Eve need to crack this matrix variant?